Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-14. (Cancelled)

15. (Currently amended) The method of claim ~~14~~ 34, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the ~~first~~ second chain of operation comprises an exclusive OR.

16. (Currently amended) The method of claim ~~14~~ 34, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the ~~first~~ second chain of operations comprises an operation of bit permutation ~~of the bits of the message or~~ of an intermediate result obtained ~~on~~ by carrying out operations of said second chain of operations ~~till the~~ preceding this operation of bit permutation ~~of the bits of the message~~.

17. (Currently amended) The method of claim ~~14~~ 34, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the ~~first~~ second chain of operations comprises an operation of indexed access to a table.

18. (Currently amended) The method of claim ~~14~~ 34, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the ~~first~~ second chain of operations comprises an operation which is stable with respect to the application of an exclusive OR function.

19. (Currently amended) The method of claim 18, wherein said corresponding part of the first chain of operations corresponding to the at least a part of the ~~first~~ second chain of operations is an operation of transfer ~~of the message or~~ of an intermediate result obtained by carrying out operations of said second chain of operations ~~until the~~ preceding this operation of transfer ~~of the message~~, from one location to another one in a storage space.

20. (Currently amended) The method of claim ~~14~~ 34, wherein the step of randomly selecting comprises identifying a series of several parts within the first chain of operations and comprises randomly selecting, for each part of said series of several parts of the first chain of operations, ~~to perform~~ said part in either ~~such part in~~ a normal state or in a complemented state.

21. (Currently amended) The method of claim ~~20~~ 34, wherein the step of randomly selecting comprises identifying a series of several operations within ~~each of said series of several parts of~~ the first chain of operations, and comprises randomly selecting, for each operation of said series of operations of ~~said series of several parts of~~ the first chain of operations, ~~to perform~~ such operation either in a normal state or in a complemented state.

22. (Currently amended) The method of claim 20, wherein the step of randomly selecting is conducted depending on the state of a random parameter generated for each ~~such~~ part of the series of several parts within this first chain of operations and comprises updating a complementation counter, and the step of selecting to output as the resultant message the result of the last operation in either in a same state or in a complemented state is decided depending on the state of the complementation counter.

23. (Currently amended) The method of claim 20, wherein the step of randomly selecting is conducted depending on the state of a random parameter generated for each ~~such~~ part of the series of several parts within this first chain of operations and comprises transmitting, for each part of said series of several parts within this ~~operation of the at least part of the~~ first chain of operations, information ~~for deciding~~ to be used during the step of outputting as the resultant message the result of the last operation in a same state of in a complemented state.

24. (Currently amended) The method of claim 20, wherein the step of randomly selecting comprises ~~the~~ a step of computing ~~of~~ a parameter which is equal to a difference between the number of times when an operation of the second ~~first~~ chain of operations ~~was performed~~ is in the same state as in the first chain of operations and the number of times when ~~other ones~~ an operation of the ~~first~~ second chain of operations of the chain ~~was performed~~ is in complemented state, and when this difference exceeds a given threshold, the ~~decision to perform~~ step of randomly selecting a next ~~operation~~ part of the series of several parts in a normal state or in a complemented state ~~or not~~ is ~~taken~~ conducted so as to decrease this difference.

25. (Currently amended) A method of performing an authentication cryptographic protocol between a server entity and a microcircuit entity in order to resist a DPA attack against the microcircuit entity during performing this authentication cryptographic protocol, comprising the steps of :

storing a DES comprising a first chain of operations in both the server entity and the microcircuit entity,

having a message exchanged between this server entity and this microcircuit entity,

having the server entity apply to the message the first chain of operations which is stored therein so as to obtain a server result,

having the microcircuit entity determine a second chain of operations from the first chain of operations which is stored in this microcircuit entity, this second chain of operations comprising a succession of operations each corresponding to a corresponding operation in the first chain of operations with each operation of the second chain of operations being the corresponding operation of the first chain of operations either in the same state or in the complemented state,

the step of having the microcircuit entity determine the second chain of operations from the first chain of operations comprising a step of randomly selecting, ~~The method of claim 14, wherein the step of randomly selecting comprises selecting randomly to perform~~ either the whole of the first chain of operations in the same state as in this first chain of operations, or the whole of the first chain of operations in complemented state selectively followed by a final complementing step,

having the microcircuit entity apply this second chain of operations to the message so as to obtain a resultant message,

comparing the resultant message obtained from the second chain of operations to the server result, and validating the authentication between the server entity and the microcircuit entity when the server result and the resultant message are identical.

26. (Currently amended) The method of claim 25, wherein the step of randomly selecting comprises computing a parameter which is the difference between the number of times when the operations of the first chain of operations were ~~performed~~ in normal state and the number of times when such operations of the first chain of operations were ~~performed~~ in a complemented state, and when this difference exceeds a given threshold, ~~a decision to perform~~ the step of randomly selecting a next one of the second chain of the operations in a normal state or in a complemented state is ~~taken~~ conducted so as to decrease this difference.

27. (Currently amended) The method of claim ~~14~~ 34, wherein the complemented state of said corresponding part of the first chain of operations corresponding to the at least a part of the ~~first~~ second chain of operations is obtained by a complementation carried out byte by byte.

28. (Currently amended) The method of claim ~~14~~ 34, wherein the complemented state of said corresponding part of the first chain of operations corresponding to the at least a part of the ~~first~~ second chain of operations is obtained by a complementation carried out bit by bit.

29. (Currently amended) The method of claim ~~14~~ 34, wherein the step of having the microcircuit entity determine ~~determining~~ the second chain of operations further comprises a step of determining a permutation of the order of successive commutative operations in the first chain of operations.

30. (Previously presented) The method of claim 29, wherein the step of determining a permutation of the order of successive commutative operations is carried out randomly.

31. (Currently amended) The method of claim 21, wherein the step of randomly selecting is conducted depending on the state of a random parameter generated for each operation of the ~~at least a part of~~ series of several operations within the first chain of operations and comprises updating a complementation counter, and the step of selecting ~~the~~ to output as the resultant message the result of the last operation in either in a same state or in a complemented state is decided depending of the state of the complementation counter.

32. (Currently amended) The method of claim ~~20~~ 21, wherein the step of randomly selecting is conducted depending of the state of a random parameter generated for each operation of the series of several ~~parts~~ operations of the first chain of operations and comprises transmitting, for each operation of the ~~at least part of~~ series of operations within the first chain of operations, information ~~for deciding~~ to be used during the step of outputting as the resultant message the result of the last operation in a same state or in a complemented state.

33. (Currently amended) The method of claim 21, wherein the step of randomly selecting comprises ~~the~~ a step of computing ~~of~~ a parameter which is equal to a difference between the number of times when an operation of the second ~~first~~ chain of operations ~~was performed~~ is in the same state as in the first chain of operations and the number of times when ~~another one~~ an operation of the ~~first~~ second chain of operations ~~of the~~

~~chain as performed~~ is in a complemented state with respect to the first chain of operations, and when the difference exceeds a given threshold, ~~a decision to perform~~ the step of randomly selecting a next operation of the second chain of operations in a normal state or in a complemented state is ~~taken~~ conducted so as to decrease this difference.

34 (New) A method of performing an authentication cryptographic protocol between a server entity and a microcircuit entity in order to resist a DPA attack against the microcircuit entity during performing this authentication cryptographic protocol, comprising the steps of :

storing a DES comprising a first chain of operations in both the server entity and the microcircuit entity,

having a message exchanged between this server entity and this microcircuit entity,

having the server entity apply to the message the first chain of operations which is stored therein so as to obtain a server result,

having the microcircuit entity determine a second chain of operations from the first chain of operations which is stored in this microcircuit entity, this second chain of operations comprising a succession of operations each corresponding to a corresponding operation in the first chain of operations with each operation of the second chain of operations being the corresponding operation of the first chain of operations either in the same state or in the complemented state,

the step of having the microcircuit entity determine the second chain of operations from the first chain of operations comprising a step of randomly selecting, for at least a part of the second chain of operations corresponding to a corresponding part of the

first chain of operations, either this at least a part of the operations of the first chain of operations in a same state as in the first chain of operations, or this at least a part of the first chain of operations in a complemented state,

the step of having the microcircuit entity determine the second chain of operations being such that at least some of the operations of this second chain of operations are in the same state as the corresponding operations in the first chain of operations whereas the other operations of this second chain of operations are in complemented state with respect to the corresponding operations of the first chain of operations,

having the microcircuit card apply this second chain of operations to the message so as to obtain a resultant message,

the step of having the microcircuit apply this second chain of operations comprising a step of selecting to output as the resultant message, depending on the step of having the microcircuit entity determine the second chain of operations, one of either the result of a last operation of the second chain of operations in a same state or the result of this last operation of the second chain of operation in a complemented state, and

comparing the resultant message obtained from the second chain of operations to the server result, and validating the authentication between the server entity and the microcircuit entity when the server result and the resultant message are identical.

35 (New) A method of performing an authentication cryptographic protocol between a server entity and a microcircuit entity in order to resist a DPA attack against the microcircuit entity during performing this authentication cryptographic protocol, comprising the steps of :

storing a DES comprising a chain of operations in both the server entity and the microcircuit entity, the operations of this chain of operations having a normal state and a complemented state,

having a message exchanged between this server entity and this microcircuit entity,

having the server entity apply to the message all operations of this chain of operations which is stored therein, so as to obtain a server result,

having the microcircuit entity apply to the message all operations of this chain of operations which is stored therein while randomly selecting, for each operation of at least a subgroup of these operations of this chain of operations, to apply this operation in either in its normal state or its complemented state, this step of having the microcircuit apply the chain of operations being such that some of the operations of this chain of operations are applied in their normal state and the other operations of this chain of operations are applied in their complemented state,

having the microcircuit select to output as a resultant message, depending on the step of having the microcircuit entity apply all operations of the chain of operations, one of either the result of a last operation of the chain of operations in a same state or this result of this last operation of this chain of operation in a complemented state, and

comparing the resultant message obtained from the microcircuit entity to the server result, and validating the authentication between the server entity and the microcircuit entity when the server result and the resultant message are identical.